

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра математической кибернетики

ШУБОДЁРОВА Любовь Александровна

**ГЕНЕРАТОР ИСТИННО СЛУЧАЙНОЙ
ПОСЛЕДОВАТЕЛЬНОСТИ В КМОП ТЕХНОЛОГИИ**

Дипломная работа

Студентки V курса специализации 1-31 03 01

на соискание квалификации “Математик. Конструктор программно-
аппаратных систем.”

Руководитель

БУХТОЯРОВ Сергей Евгеньевич

доцент кафедры математической
кибернетики

кандидат физико-математических
наук

Допустить к защите
Заведующий кафедрой,
профессор

“ ___ ” _____ 20__ г.

Минск, 2016

РЕФЕРАТ ДИПЛОМНОЙ РАБОТЫ

Дипломная работа содержит

- 41 страницу,
- 24 иллюстрации (рисунка),
- 3 таблицы,
- 13 использованных источников.

Ключевые слова: ГЕНЕРАТОР ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ, АППАРАТНЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ, КОЛЬЦЕВОЙ ГЕНЕРАТОР, ОПЕРАЦИОННЫЙ УСИЛИТЕЛЬ.

В дипломной работе рассматривается разработка ГИСЧ на основе кольцевых генераторов и ГИСЧ на основе операционного усилителя.

Целью дипломной работы является разработка нескольких вариантов реализации генератора истинно случайных чисел на КМОП элементной базе с проектной нормой 0.18 мкм.

В дипломной работе получены следующие результаты:

- 1) Разработаны электрические схемы ГИСЧ на основе кольцевых генераторов на КМОП технологии с проектной нормой 0,18 мкм;
- 2) Разработаны электрические схемы ОУ и ГИСЧ на его основе на КМОП технологии с проектной нормой 0,18 мкм;
- 3) Оптимизированы параметры схем и проведен спектральный анализ.

Дипломная работа выполнена автором самостоятельно.

РЭФЕРАТ ДЫПЛОМНАЙ РАБОТЫ

Дыпломная работа ўтрымлівае:

- 41 старонку,
- 24 ілюстрацый (малюнкаў),
- 3 табліцы,
- 13 выкарыстаных крыніц.

Ключавыя словы: ГЕНЕРАТАР САПРАЎДНА ВЫПАДКОВЫХ ЛІЧБАЎ, АПАРАТНЫ ГЕНЕРАТАР ВЫПАДКОВЫХ ЛІЧБАЎ, КАЛЬЦАВЫ ГЕНЕРАТАР, АПЕРАЦЫЙНЫ УЗМАЦНЯЛЬНІК.

У дыпломнай рабоце разглядаецца распрацоўка ГСВЛ на аснове кальцавых генератараў і ГСВЛ на аснове аперацыйнага ўзмацняльніка.

Мэтай дыпломнай работы з'яўляецца распрацоўка некалькіх варыянтаў рэалізацыі генератара праўдзіва выпадковых лічбаў на КМОП элементнай базе з праектнай нормай 0.18 мкм.

У дыпломнай рабоце атрыманы наступныя вынікі:

- 1) Распрацованы электрычныя схемы ГСВЛ на аснове кальцавых генератараў на КМОП тэхналогіі з праектнай нормай 0.18 мкм;
- 2) Распрацованы электрычныя схемы аперацыйнага ўзмацняльніка і ГСВЛ на яго аснове на КМОП тэхналогіі з праектнай нормай 0.18 мкм;
- 3) Аптымізаваны параметры схем і праведзены спэктральны аналіз.

Дыпломная праца выканана аўтарам самастойна.

ABSTRACT OF THE THESIS

This thesis consist of:

- 41 pages,
- 24 illustrations (figures),
- 3 tables,
- 13 used sources.

Keywords: TRUE RANDOM NUMBER GENERATOR, HARDWARE RANDOM NUMBER GENERATOR, RING OSCILLATOR, OPERATING AMPLIFIER.

TRNG based on ring oscillators and TRNG based on OpAmp are considers in this thesis work.

Goal of this work is development of TRNG based on ring oscillators and TRNG based on the operational amplifier. The aim of thesis is to develop a number of embodiments of a true random number generator in CMOS element base with the design rule of 0.18 microns.

In thesis work following results were obtained:

- 1) Developed electric circuits of TRNG based on ring oscillators in CMOS technology with a design rule of 0.18 microns;
- 2) Developed electrical circuits of OA and TRNG on its basis in the CMOS technology with a design rule of 0.18 microns;
- 3) Circuits parameters are optimized and the spectral analysis is carried out.

Thesis is completed by author herself.